WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Role of Block chain in Strengthening IoT Security and Data Integrity

Mrs. Yogita Patgar

Assistant Professor SDM College of Business Management,Mangalore
yogitapatgar@gmail.com
9742684278

ABSTRACT

Blockchain can greatly assist in strengthening the security and data integrity of IoT (Internet of Things) systems. Its open and decentralized nature helps to balance the disadvantages of traditional centralized IoT systems, which can be vulnerable to cyber-attacks and single points of failure. Enhancing blockchain's features helps IoT systems to offer more security, improved data integrity, and more participant confidence. We examine how blockchain's decentralized and unchangeable ledger can enhance data integrity and security of IoT. First, we propose a unified IoT system based on blockchain to guarantee sensing data integrity, so providing device owners a whole, unchangeable log and straightforward access to their devices. Smart contracts on this platform help to specify the business logic and rules, therefore enabling real-time monitoring and control. Second, we offer a novel blockchain-based data checking system specifically designed for resource-constrained IoT devices. Using a stochastic approach to randomly select cooperative nodes for data broadcasting, this system enhances security and distributes the load among edge nodes. A lightweight mining technique increases performance even more by focusing block generation on edge nodes. Using Raspberry Pi devices and Hyper ledger Fabric, we demonstrate the effectiveness and scalability of the proposed solutions by means of proof-of-concept implementations and performance benchmarks. Our research underlines the remarkable potential of blockchain to improve data integrity, bolster IoT security, and pave the way for more robust and dependable IoT deployments. We especially show that even with a great number of compromised nodes, our stochastic data checking technique can achieve high levels of data integrity. .

Keywords: Block chain, IoT, Data Integrity, leveraging

Introduction

Block chain is predicted to greatly affect the information technology revolution. A distributed ledger technology, blockchain offers characteristics including immutability, decentralization, and openness that could enhance data integrity in IoT systems. Sensor data from devices can be securely stored on a blockchain in IoT environments, where each block is cryptographically linked to the preceding one, creating a tamper-proof record of transactions and guaranteeing the integrity and reliability of the collected data. Blockchain also provides improved access control, hence safeguarding user privacy and preventing unlawful data breaches. By eliminating the need for a central authority, it encourages decentralized trust and lowers the likelihood of security breaches. Still unresolved are problems including scalability and privacy.

Blockchain for IoT Security

The main characteristics of blockchain complementing well for addressing IoT security concerns:

- **Immutability:** Once data is recorded on the blockchain, it cannot be changed or deleted, therefore guaranteeing data integrity and auditability.
- **Decentralization:** Decentralization: Blockchain removes single points of failure by its distributed character, therefore reinforcing the system against attacks.
- **Transparency:** Every blockchain transaction is publicly visible, therefore promoting confidence and responsibility.
- **Smart Contracts:** Smart contracts can automate security processes, implement access control policies, and allow safe data sharing.

IoT Security Challenges

- **Data Integrity:** Large amounts of data generated by IoT devices can be vulnerable to manipulation during transmission or storage. Data integrity is fundamental to good decision-making.

- **Access Control:** Controlling access to IoT devices and data is essential to prevent unauthorized access and malicious activities. Traditional access control mechanisms may not be scalable or adaptable to the dynamic nature of IoT.

- **Authentication:** Preventing unlawful access and hostile activities depends on controlling access to IoT devices and data. Traditional access control systems may not be scalable or adaptable to the dynamic nature of IoT.IoT device and user identity verification determines illegal access prevention and safe communication guarantee. Devices with limited resources call for simple authentication mechanisms.
- **Privacy:**Because they handle and collect sensitive personal data, IoT devices create significant privacy concerns. Privacy of the user is most crucial. .
- **Scalability:** Securing billions of linked devices calls for scalable solutions able to handle the growing volume of data and transac tions. .

Strengths and Limitations

- **Scalability**: Processing a large number of blockchain transactions can be time-consuming and computationally intensive.
- **Resource Constraints**: Running blockchain directly on many IoT devices is challenging since they have restricted processing power and memory.
- **Privacy Concerns**: Though blockchain can enhance privacy in some areas, its transparency can also cause privacy problems if not managed correctly.

Research Challenges and Future Directions

- **Scalability Solutions**: It is absolutely crucial to create scalable blockchain solutions able to manage the vast data volumes generated by IoT devices. .
- **Lightweight-Blockchain Implementations** : Developing lightweight blockchain implementations deployable on resource-constrained IoT devices is absolutely vital.
- **Privacy-Preserving-Techniques**: Developing privacy-preserving policies that can be combined with blockchain to protect user privacy is absolutely vital.
- **Interoperability**:Seamless integration relies on guaranteeing interoperability between many IoT devices and blockchain systems.

Conclusion

For data integrity and IoT security, blockchain technology might be revolutionary. Its inherent characteristics of openness, decentralization, and unchangeability offer a solid foundation for building dependable and safe IoT ecosystems. Though challenges remain, ongoing research and development are addressing these limitations.As it ages and becomes more scalable and efficient, blockchain technology will play an ever more vital role in safeguarding the always growing IoT universe.

REFERENCES:

1. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media. Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017). Blockchain-oriented software engineering: Challenges and new directions.
2. Agrawal, T. K., Kumar, V., Pal, R., Wang, L & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry.Computers & Industrial Engineering, 154,107130.
3. Liang, X.; Zhao, J.; Shetty, S.; Li, D. Towards data assurance and resilience in IoT using blockchain. In Proceedings of the IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 261–266.
4. B. Tian et al., "A Blockchain-based Trusted Testing System of Electric Power Materials," 2021 IEEE 29th International Conference on Network Protocols (ICNP), Dallas, TX, USA, 2021, pp. 1-5, doi:10.1109/ICNP52444.2021.9651966